

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554

RECEIVED  
FEB 10 1994  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554

In the Matter of )  
 )  
Policies and Rules ) CC Docket No. 93-292  
Concerning Toll Fraud )

REPLY COMMENTS OF  
THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Cellular Telecommunications Industry Association ("CTIA") hereby submits its reply to comments on the Notice of Proposed Rule Making in the above-captioned proceeding.<sup>1/</sup> In its comments,<sup>2/</sup> CTIA endorsed the Commission's proposal that liability for fraud should rest with the entity most able to control it, and supported the Commission's proposal to strengthen the wording of Rule 22.915 originally set forth in the Commission's Part 22 rewrite proceeding, Revision of Part 22 of the Commission's Rules Governing the Public Mobile Service, Notice of Proposed Rulemaking, 7 FCC Rcd 3658, 3741 (1992). CTIA also urged the Commission to support legislation that would modify 18 U.S.C. Section 1029, the federal criminal statute that makes it a crime to use a counterfeit access device to commit fraud, so as to clearly extend the scope of the statute to anyone who uses a fraudulent account number to access cellular and

---

<sup>1/</sup>In the Matter of Policies and Rules Concerning Toll Fraud, Notice of Proposed Rule Making, CC Docket No. 93-292 FCC 93-496, 8 FCC Rcd [ ] (released Dec. 2, 1993) ("Notice").

<sup>2/</sup>Comments of the Cellular Telecommunications Industry Association, CC Docket No. 93-292 (Jan. 14, 1994).

No. of Copies rec'd  
List ABCDE

204

commercial mobile radio services. In addition, CTIA endorsed additional legislation that would make altering an ESN a federal crime.

To have viable commercial mobile radio services, it is essential that all mobile units have a unique identification number.<sup>3/</sup> Protecting the integrity of each mobile unit's unique ESN provides cellular and other wireless carriers with the ability to establish validation processes for the provision of service to subscribers. Effective validation is necessary to bill customers for their use of wireless services, and is essential in combatting access fraud, since cellular systems sort legitimate users from illegitimate users based on a mobile unit's ESN.

Both McCaw and Sprint, in their comments, note that the counterfeiting of cellular phones is often accomplished without actually changing (or removing) the unique factory-set ESN stored in each mobile unit. Instead, the mobile unit's operating software is compromised and the phone is made to transmit a counterfeit ESN stored in an alternative memory location. Both Section 22.929, and any legislation proposed to address wireless access fraud, should make clear that it is a violation of the Part 22 rules, and federal law, to modify a mobile unit in any way that causes the phone to transmit an identification code

---

<sup>3/</sup>Cellular mobile units use both an Electronic Serial Number ("ESN") and a Mobile Identification Number ("MIN") to uniquely identify each unit. See CTIA Comments at 5.

other than the unique factory-set ESN.<sup>4/</sup> It is of no import that a factory-set ESN technically may still reside in a mobile unit if the device has been tampered with and made to transmit a counterfeit ESN to gain access to a wireless service. Therefore, the Commission should make clear that both its existing rules, as well as its proposed rules, prohibit any tampering with a mobile unit which enables the unit to transmit any code other than the unique factory-set ESN.<sup>5/</sup> In addition, as Southern New England Telecommunications Corporation urges in its comments, the Commission's antitampering rules should be codified as part of the federal criminal code.<sup>6/</sup>

As previously noted, CTIA agrees with the Commission that liability for fraud should rest with the entity most able to control it. In a multi-carrier environment where the risk of fraud is shared, the Commission should make a carrier responsible for the fraudulent activity that the carrier can control, at least theoretically, or where the carrier has a direct relationship with the user.

AT&T, MCI, and the National Cellular Resellers Association, each support the adoption of rules that place all of the

---

<sup>4/</sup>Sprint Comments, at 12-13; McCaw Comments at 9-12.

<sup>5/</sup>In addition, the type acceptance rules for cellular mobile units should require manufacturers to design their units so that any tampering with the unit that permits the unit to transmit a code other than the factory-set ESN shall render the unit inoperative. For example, Sprint proposes that the ESN should not be modifiable via the phone's data port. Sprint Comments at 13.

<sup>6/</sup>SNET Comments at 11.

liability for fraudulent cellular calls exclusively on cellular carriers. As described below, there are two fundamental flaws with such proposals. First, both resellers and interexchange carriers have the ability to control some types of cellular fraud, and therefore should share the risk; and second, a cellular reseller and an interexchange carrier (in an equal access environment) each possess a direct relationship with the customer that they deny to cellular carriers. To create the appropriate incentives to combat fraud, interexchange carriers and cellular resellers should be liable for fraud that they can control. Existing arrangements in the cellular industry already reflect this basic theory.

As Southern New England Telecommunications Corporation notes in its Comments,

End-users have the responsibility to: 1) protect the accessibility to the mobile unit as well as any documentation which contains their ESN/MIN combination; 2) conform to reasonable precautionary methods and features (PINS, A-KEY, call restrictions) as made available by the carrier; 3) immediately report such items as stolen units, unrecognized calls on bills, unauthorized use of the unit, and service problems which could lead to or be the result of fraudulent calls; and 4) not utilize unauthorized or illegally modified access equipment.<sup>7/</sup>

Since cellular resellers, not cellular carriers, have the account relationship with their customers, a cellular carrier has no ability to control fraud associated with these types of

---

<sup>7/</sup>SNET Comments at 10-11.

activities. Such control resides exclusively with the cellular reseller.

Similarly, if a cellular carrier (or interexchange carrier) detects suspicious activity associated with a cellular reseller's customer, the cellular carrier must rely on the cellular reseller to contact the customer and determine whether the activity is authorized or fraudulent. Cellular carriers do not know the identity of individual customers who order service through cellular resellers, and have no way of contacting such customers directly. Thus, if suspicious activity is detected at night or over a weekend, and the cellular reseller has not established a 24 hour customer service contact, the initial contact can be delayed while fraudulent calls accumulate.

Both cellular resellers and interexchange carriers have made clear that they do not want cellular carriers interfering with what they see as their exclusive relationship with their customers. Since determining whether to continue or suspend a customer's service goes to the heart of the customer relationship, if the Commission were to limit the liability of cellular resellers and interexchange carriers for fraudulent calling, the FCC also should make clear that a cellular carrier has the right to unilaterally suspend a customer's service in order to protect itself against liability for fraudulent calling.

As CTIA and McCaw note in their comments, interexchange carriers do have the ability to monitor calling activity for suspicious and fraudulent patterns of unauthorized calls. That

ability, coupled with an account relationship, is sufficient to make the interexchange carrier jointly liable for fraud.

Accordingly, if there is fraudulent calling, the long distance losses should be borne by the interexchange carrier, while cellular air time charges are absorbed by the cellular carrier.

The Commission should preserve existing shared liability arrangements, and extend the principle wherever feasible. A federal policy of shared fraud liability will provide customers and carriers whose facilities and equipment are involved in handling a fraudulent call with a strong incentive to deploy anti-fraud measures and to take other appropriate steps to ensure that fraud is minimized.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read "Michael F. Altschul", is written over a horizontal line.

Michael F. Altschul  
Cellular Telecommunications  
Industry Association  
1250 Connecticut Ave., N.W.  
Suite 200  
Washington, D.C. 20036  
(202) 785-0081


DATED: February 10, 1994

Certificate of Service

I, Michael F. Altschul, hereby certify that on this 10th day of February, 1994, copies of the foregoing Reply Comments of the Cellular Telecommunications Industry Association were served by hand delivery upon the following parties:

William F. Caton  
Secretary  
Federal Communications Commission  
1919 M Street, N.W., Room 222  
Washington, D.C. 20554

International Transcript Service  
1919 M Street, N.W., Room 246  
Washington, D.C. 20554

---

Michael F. Altschul